EXHIBIT A

IN THE COUNTY COURT OF THE 11TH JUDICIAL CIRCUIT IN AND FOR MIAMI-DADE COUNTY, FLORIDA

Sergio Salani,

Plaintiff,

v.

AT&T Mobility, LLC,

Defendant.
_____/

CASE NO.: 2022-047421-SP-25

BAR NO.: 121673

SECOND AMENDED STATEMENT OF CLAIM

Plaintiff, Sergio Salani, through its undersigned counsel, hereby files this Third Amended Statement of Claim against Defendant, AT&T, Mobility, LLC ("AT&T MOBILITY, LLC"), and further alleges as follows:

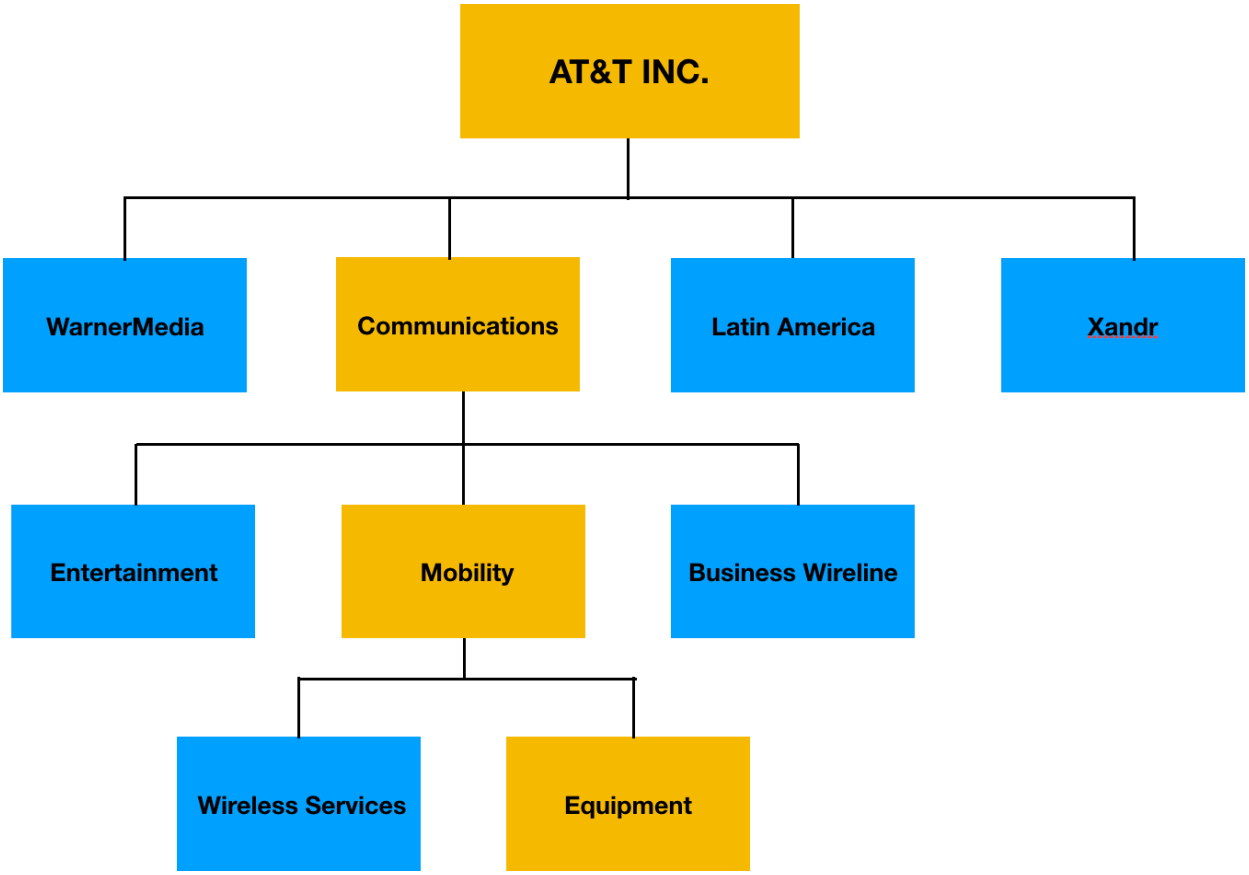
GENERAL ALLEGATIONS

1. This is an action against AT&T for damages for $8,000, exclusive of interest, attorney's fees, and costs.
2. Plaintiff is a customer of AT&T Mobility, LLC, a Florida consumer with cell number XXX-XX9-8349.
3. Plaintiff is not in possession of the specific wireless agreement with Defendant.
4. AT&T MOBILITY, LLC is a foreign limited liability company licensed and doing business in Miami-Dade County, Florida subject to the jurisdiction of this Court.
5. Venue is proper in Miami-Dade County, Florida.
6. Plaintiff has complied with all conditions precedent to filing this action or said conditions have been waived by AT&T Mobility, LLC.

7. This claim is not preempted by any federal law or statute.
8. This action is not a class action.
9. According to court filings made by AT&T MOBILITY, LLC in federal court, it is a nongovernmental limited liability company that has no parent company, but its members are BellSouth Mobile Data, Inc.; SBC Long Distance, LLC; and SBC Tower Holdings LLC. Those entities (and thus AT&T MOBILITY, LLC) are all indirectly wholly owned by AT&T Inc., which is the only publicly held company with a 10 percent or greater ownership stake in them.
10. AT&T, Inc. reports its consolidated business results, and breaks out selected disclosures for its major operating segments. Their segments are strategic business units that offer different products and services over various technology platforms and/or in different geographies that are managed accordingly. They analyze the operating segments based on segment contribution, which consists of operating income, excluding acquisition-related costs and other significant items, and equity in net income (loss) of affiliates for investments managed within each operating segment.
11. There are four reportable segments of AT&T, Inc.: (1) Communications, (2) Warner Media, (3) Latin America and (4) Xandr. AT&T MOBILITY, LLC is a major retailer of smartphones and provider of wireless broadband internet access service for smartphones.
12. Smartphone owners use mobile data for, including but not limited to, sending and receiving email, using GPS navigation, watching and streaming video, and browsing the internet. AT&T MOBILITY, LLC is a major retailer of smartphones and provider of wireless broadband internet access service for smartphones (“mobile data”). Smartphone owners

use mobile data for, including but not limited to, sending and receiving email, using GPS navigation, watching and streaming video, and browsing the internet.

13. AT&T MOBILITY, LLC's place in AT&T Inc corporate structure can be identified as follows:



14. The Communications segment provides wireless and wireline telecom, video and broadband services to consumers located in the U.S. or in U.S. territories and businesses globally. Communications services and products are marketed under the AT&T, Cricket, AT&T PREPAID and DIRECTV brand names. The Communications segment provided approximately 84% of 2018 segment operating revenues and 84% of our 2018 total segment contribution. This segment contains the Mobility, Entertainment Group and

Business Wireline business units.

15. AT&T Mobility, LLC's previous in court public admissions (filed by its corporate counsel, Patricia Cruz, Esq.) has admitted to anit-consumer behavior, see the cases of Erin Young v. AT&T Mobility, LLC, Case No. 2019-2027-SP-26, EFiling#87601121 or Tamara Crespo v. AT&T Mobility, LLC, Case No. 2019-2026-SP26, E-Filing#87600869 both of which alleged AT&T's violation of FDUTPA for illegal data throttling and bogus administrative fee, is further evidence of AT&T Mobility, LLC's illegal, immoral and unethical conduct toward consumers.

COUNT I - NEGLIGENCE FOR DATA BREACH

16. Plaintiff re-alleges, restates, and incorporates the allegations contained in paragraphs one (1) through fifteen (15) as fully set forth herein.

17. AT&T learned that a well-known threat actor claimed to be selling a database containing the personal information of over 70 million AT&T customers. This information included customers' names, addresses, phone numbers, Social Security numbers, and dates of birth. But instead of investigating the source and cause of the massive breach, AT&T denied the allegations, ignored the issue, and continued with operations. AT&T told one media outlet that "the information that appeared in an internet chat room does not appear to have come from our systems." And when questioned about its vendors, AT&T chose not to speculate: "Given this information did not come from us, we can't speculate on where it came from or whether it is valid." AT&T attempted to fully wash its hands of the disaster.

18. The same customer data is no longer just for sale; it has been fully exposed on the Dark Web. And after years of denial, AT&T has changed its tune. AT&T finally admitted that

approximately 73 million former and current AT&T customers' personal and sensitive information was released onto the Dark Web (the "Data Breach"), including Plaintiff's information.

19. According to AT&T, customers' impacted information included a combination of their "full name, email address, mailing address, phone number, social security number, date of birth, and AT&T account number and passcode" (collectively, "PII"), which AT&T collected as a condition for use of its services. This recent revelation marks a concerning turn of events.

20. Equally troubling is that AT&T still appears clueless as to the source of the breach. One would hope that – in nearly three years – a telecom giant like AT&T would have conducted a "robust investigation" into the data leak to determine who was responsible, where the data originated from, which customers were impacted, how the Data Breach occurred, and other key factors. But it did not. Had it done so, the 73 million customers could have attempted to adequately protect themselves. Instead, AT&T remained willfully blind.

21. This Data Breach and resulting injuries occurred because AT&T failed to implement reasonable security procedures and practices (including failing to exercise appropriate managerial control over third-party partner's data security), failed to disclose material facts surround its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

22. In connection with providing its wireless services, AT&T required Plaintiff to provide personal information, including but not limited to names, addresses, Social Security numbers, and dates of birth.

23. Given the amount and sensitive nature of the data it collects, AT&T maintains policies explaining its privacy practices handling consumers' personal information. Through these policies, AT&T represents to consumers and the public that it possesses robust security features to protect PII and it they their responsibility to protect PII seriously.

24. Given AT&T's avowed experience in its field handling highly sensitive information, it understood the need to protect consumers' PII and prioritize data security.

25. AT&T admitted that its data security was breached and acknowledged the legitimacy of the leaked customer data:

> AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance of the data set, which includes personal information such as social security numbers, the source of the data is still being assessed.
>
> AT&T has launched a robust investigation supported by internal and external cybersecurity experts. Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders.
>
> Currently, AT&T does not have evidence of unauthorized access to its systems resulting in exfiltration of the data set. The company is communicating proactively with those impacted and will be offering credit monitoring at our expense where applicable. We encourage current and former customers with questions to visit www.att.com/accountsafety for more information.
>
> As of today, this incident has not had a material impact on AT&T's operations.

26. AT&T had a duty to protect Plaintiff's private information and has breached that duty.

27. But AT&T, like any company of its size that stores massive amounts of sensitive PII,

should have had robust protections in place to detect and terminate a successful intrusion long before access and exposure of customer data. AT&T also should have exercised appropriate managerial control over their third-party partners' data security when it knew these partners stored its customers' PII in the course of carry out the business of their partnership. AT&T's failure to prevent the breach is inexcusable given its knowledge that it and its affiliates are prime targets for cyberattacks.

28. In 2022, the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) co-authored the joint Cybersecurity Advisory explicitly highlighting [t]elecommunications and network service provider targeting" by cyber actors. The Advisory explains how cyber actors exploit and access telecommunication organizations and network service providers though the use of open-source tools "that allows for the scanning of IP addresses for vulnerabilities." Once these cyber actors gain an initial foothold, they identify "critical users and infrastructure including systems critical to maintaining the security of authentication, authorization, and accounting."

29. Thus, whether the data breach occurred through AT&T's own systems or its third-party vendors, AT&T was responsible for the protection of Plaintiff's PII.

30. And AT&T recognized these risks in its own regulatory filings with the SEC.

31. If not through its own history, AT&T surely understood the risk from its competitors. Considering recent high profile data breaches at other telecommunications companies, such as Xfinity (36,000,000 impacted, announced December 2023); T-Mobile (37,000,000 impacted, announced January 2023); and US-Cellular (52,000 impacted, announced March 2023), among others, AT&T knew or should have known

that its data and consumers' PII would be, or had already been, targeted by cybercriminals.

32. To prevent unauthorized access, CISA encourages organizations to:

- Conduct regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patch and update software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensure devices are properly configured and that security features are enabled;
- Employ best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disable operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.

33. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.

34. Consequently, AT&T knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if their data security system was

breached, including the significant costs that would be imposed on customers as a result of a breach.

35. But despite all of the publicly available knowledge of the continued compromises of PII and despite holding the PII of millions of customers, AT&T failed to use reasonable care in maintaining the privacy and security of the PII of Plaintiff.

36. Had AT&T implemented industry standard security measures, adequately invested in data security, and promptly investigated cybersecurity issues, unauthorized parties likely would not have been able to access AT&T's or its third- party vendors' systems and the Data Breach would have been prevented or much smaller in scope.

37. The PII of consumers, including Plaintiff, remains of high value to criminals, as evidenced by the continued sale and trade of such information on underground markets found on the "dark web"— which is a part of the internet that is intentionally hidden and inaccessible through standard web browsers

38. Data sets that include PII demand a much higher price on the black market. For example, the information likely exposed in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[25] The information likely disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

39. There is also an active and robust *legitimate* market for PII. In 2021, the data brokering industry alone was valued at $319 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers

or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.

40. Because their PII has independent value, Plaintiff must take measures to protect it including by, as AT&T's online notice instructs, placing "alerts" with credit reporting agencies, changing passcodes, and reviewing and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

41. In connection with obtaining AT&T's services, Plaintiff was required to provide highly sensitive personal information, such as his contact information, date of birth, Social Security number, and so on. AT&T also prompted Plaintiff to create login credentials to access his accounts.

42. In the regular course of business, AT&T shared Plaintiff's information with several third-party partners whom AT&T was obligated to verify their data security practices because those third parties stored the information AT&T collected.

43. Plaintiff has confirmed that it was a victim of the Data Breach.

44. Because AT&T continues to store and share PII in the regular course of its business, Plaintiff has a continuing interest in ensuring that the PII is protected and safeguarded from additional authorized access.

45. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (FTC) has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.

46. The FTC's publication Protecting Personal Information: A Guide for Business sets

forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.

47. Among other things, the guidelines note that businesses should (a) protect the customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.

48. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry- tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

49. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. AT&T was fully aware of its obligation to implement and use reasonable measures to protect customers' PII but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. AT&T's failure to

employ reasonable measures to protect against unauthorized access to customer information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

51. Though limited detail is available on the Data Breach, how it occurred or the entity the information originated from, AT&T's failure to safeguard customers' PII suggests AT&T failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, user-activity monitoring, data-loss prevention, encryption, intrusion detection and prevention, and exercising managerial control over third-party vendors' cybersecurity practices.

52. AT&T's failure to keep Plaintiff's PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, date of birth, Social Security numbers, and potentially other sensitive information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff now and into the indefinite future

53. As a result, Plaintiff has suffered injury including as the information has already been published to the Dark Web available for any cybercriminal to misuse.

54. As discussed above, the PII likely exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government

benefits, obtain government IDs, or create “synthetic identities.

55. Further, malicious actors may wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

56. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. According to the Government Accountability Office, which conducted a study regarding data breaches: “law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. The unauthorized disclosure of the sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.

57. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a

victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense. And here, Plaintiff's PII is already available to criminal actors on the dark web.

58. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff has and will continue to suffer harm for which it is entitled to damages, including, but not limited to, the following the unconsented disclosure of confidential information to a third party;

- losing the value of the explicit and implicit promises of data security;
- identity theft and fraud resulting from the theft of their PII;
- costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;
- unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and
- the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

59. Plaintiff has a direct interest in AT&T's promises and duties to protect its PII, *i.e.,* that AT&T *not increase* their risk of identity theft and fraud. Because AT&T failed to live up to its promises and duties in this respect, Plaintiff seeks the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by AT&T's wrongful conduct.

60. Through this remedy, Plaintiff seeks to restore close to the same position as they would have occupied but for AT&T's wrongful conduct, namely their failure to adequately protect the information. Plaintiff further seeks to recover the value of the unauthorized access to their PII permitted through AT&T's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology.

61. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.,* a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non- practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff has a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions.

62. Defendant AT&T required Plaintiff's PII as a condition to receiving AT&T's services. AT&T collected and stored this PII for commercial gain. AT&T collected, stored, and through its partnership with third- party vendors, shared the data with these vendors for providing AT&T's services as well as commercial gain.

63. AT&T owed a duty of care to Plaintiff to provide adequate data security, consistent with industry standards, to ensure that AT&T's and its vendors' systems and networks adequately protected the PII

64. AT&T owed a duty of care to Plaintiff so as to alleviate the risk of compromising Plaintiff's PII.

65. AT&T duty to use reasonable care in protecting PII arises because of the parties' relationship, as well as common law and federal law, including the FTC regulations described above and AT&T's own policies and promises regarding privacy and data security.

66. AT&T knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location for the purpose of carrying out the business of the partnership, its vendors' vulnerability to network attacks, and the importance of adequate security.

67. AT&T breached its duty to Plaintiff in numerous ways, as described herein, including by:

- Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff;
- Failing to ensure its vendors implemented adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff;
- Failing to supervise its vendors regarding vendors' data security systems, protocols, and practices when it knew or should have known those systems, protocols, and practices were inadequate;
- Failing to comply with industry standard data security measures for the

telecommunications industry leading up to the Data Breach;

- Failing to comply with its own privacy policies;
- Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;
- Failing to adequately monitor, evaluate, and ensure the security of their vendors' network and systems;
- Failing to recognize in a timely manner that PII had been compromised; and
- Failing to timely and adequately disclose the Data Breach.

68. Plaintiff's PII would not have been compromised but for AT&T's wrongful and negligent breach of its duties

69. AT&T's failure to take proper security measures to protect the sensitive PII of Plaintiff as described herein, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access, copying, and exfiltrating of PII by unauthorized third parties. Given that telecommunications businesses are prime targets for hackers, of having its PII misused or disclosed if not adequately protected by AT&T.

70. It was also foreseeable that AT&T's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff.

71. As a direct and proximate result of AT&T's conduct, Plaintiff has suffered damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with

addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) potential time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) the continued risk to their PII, which remains in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect it; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (viii) any nominal damages that may be awarded.

WHEREFORE, Plaintiff respectfully requests that this Court grant judgment in its favor and against AT&T and any other relief the Court deems just and proper including attorney's fees and costs.

COUNT II-VIOLATION OF FDUTPA FOR DATA BREACH

72. Plaintiff re-alleges, restates, and incorporates the allegations contained in paragraphs one (1) through seventy-one (71) as fully set forth herein.

73. Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of FDUTPA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's Sensitive Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Sensitive Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's Sensitive Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's Sensitive Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

74. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Sensitive Information.

75. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violated FDUTPA.

76. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Sensitive Information of Plaintiff, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

77. The aforesaid conduct constitutes a violation of FDUTPA, Fla. Stat. § 501.204, in that it is a restraint on trade or commerce and was furthermore unconscionable, unfair and deceptive.

78. Defendant's implied and express representations that it would adequately safeguard Plaintiff's Sensitive Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of Fla. Stat. § 501.202(2).

79. Most, if not all, of the alleged misrepresentations and omissions by AT&T complained of herein that led to inadequate safety measures to protect patient information occurred within or were approved within Florida.

80. AT&T's representations that it would adequately safeguard Plaintiff's Sensitive Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Fla. Stat. § 501.204(1)..

81. AT&T knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant claims that it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain the personal information as represented, in violation of Fla. Stat. § 501.171.

82. These violations have caused actual damages to Plaintiff

83. Plaintiff, brings this action under the Deceptive and Unfair Trade Practices Act to seek such her actual damages incurred for violations and to recover costs of this action, including reasonable attorneys' fees and costs.

WHEREFORE, Plaintiff respectfully requests that this Court grant judgment in its favor and against AT&T for damages, interest, court costs, attorney's fees, and any other relief the Court deems just and proper.

COUNT III - BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING

84. Plaintiff re-alleges, restates and incorporates the allegations contained in paragraphs one (1) through seventy-one (71) above, and further alleges as follows:

85. Plaintiff had a wireless agreement with AT&T wherein Plaintiff had a reasonable expectation of performance of the agreement by AT&T to keep Plaintiff's PII safe

86. As part of these transactions, AT&T agreed to safeguard and protect the PII of Plaintiff. Implicit in these transactions between AT&T and Plaintiff was the obligation that AT&T would use the PII for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

87. Additionally, AT&T implicitly promised to retain this PII only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII of Plaintiff from unauthorized disclosure or access.

88. Plaintiff had a reasonable expectation that AT&T's data security practices and policies, including adequate managerial supervision of vendors' data security, were

reasonable and consistent with industry standards believed that AT&T would use part of the monies paid to AT&T to fund adequate and reasonable data security practices to protect their PII.

89. . The safeguarding of Plaintiff's PII was critical to realizing the intent of the parties.

90. AT&T breached its implied contract with Plaintiff by failing to reasonably safeguard and protect Plaintiff's PII, which was compromised as a result of the Data Breach.

91. As a direct and proximate result of AT&T's breaches, Plaintiff sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Alternatively, Plaintiff seeks an award of nominal damages.

92. AT&T has breached the express terms of the wireless agreement.

93. As a result of AT&T's breach of implied covenant of good faith and fair dealing, Plaintiff has been damaged.

WHEREFORE, Plaintiff respectfully requests that this Court grant judgment in its favor and against AT&T for compensatory damages, nominal damages, interest, court costs, and any other relief the Court deems just and proper.

COUNT IV – ACTION FOR DECLARATORY RELIEF AND/OR INJUNCTIVE RELIEF UNDER FDUTPA – DATA BREACH

94. Plaintiff re-alleges, restates, and incorporates the allegations contained in paragraphs one (1) through seventy (70), above, and further alleges as follows:

95. Under the FDUTPA, without regard to any other remedy or relief to which a person is entitled, anyone aggrieved by a violation of this part may bring an action to obtain a declaratory judgment that an act or practice violates this part and to enjoin a person who has violated, is violating, or is otherwise likely to violate 501.201 et. seq. See

Fla. Stat. §501.211(1). Plaintiff is an aggrieved consumer whose rights have been, are being, or will be adversely affected, by AT&T MOBILITY, LLC.'s violation of FDUTPA--meaning an unfair or deceptive practice which is injurious to consumers, including Plaintiff.

96. Pursuant to AT&T MOBILITY, LLC's above-described acts or practices of placing a improperly safeguarding Plaintiff's account, AT&T MOBILITY, LLC violated the FDUTPA.

97. Plaintiff seeks a declaratory judgment that AT&T MOBILITY, LLC's acts or practices have violated the FDUTPA.

98. Plaintiff seeks to determine whether the FDUTPA prohibits AT&T MOBILITY, LLC from continuing to allow Plaintiff's PII to be distributed and left unsafeguarded in the future.

99. There is a bona fide dispute between the parties. Plaintiff has a justiciable question as to the existence or non-existence of some right, status, immunity, power, or privilege, or some fact upon which their claim may depend.

100. here is a bona fide, actual, and present need for the declaration.

101. Plaintiff has retained the undersigned to represent it in this action and pay a reasonable fee for said legal services.

WHEREFORE, Plaintiff respectfully requests that this Court grant declaratory judgment and/or injunctive relief in its favor and against AT&T MOBILITY, LLC, court costs, attorney's fees pursuant to Section 501.2105, Florida Statutes, and any other relief the Court deems just and proper.

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that a true and correct copy of the foregoing was served via e-mail this this this January 17, 2025 to: all counsel of record.

Beighley, Myrick, Udell, Lynne & Zeichman PA
Attorneys for Plaintiff
2601 S. Bayshore Drive, Suite 770
Miami, FL 33133
(305) 349-3930 – Phone

By: _/s/ *Maury L. Udell*_____
Maury L. Udell, Esquire
mudell@bmulaw.com
Fla. Bar 121673